IN THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Please amend the claims as follows:

1. (Currently Amended) A computer readable medium having stored thereon data representing instructions that, when executed by a processor, cause the processor to perform operations comprising:

generating a tag describing an object captured during transmission from an origination address to a destination address, ~~wherein the object is captured and the captured object is a plurality of packets that are broken down by a capture system and then reassembled, and~~ wherein the tag includes,

a source address field to indicate an origination address of the object,

a destination address field to indicate a destination address of the object,

a source port field to indicate an origination port of the object,

a destination port field to indicate a destination port of the object,

a content field to indicate a content type from a plurality of content types identifying a type of content contained in the object, and

a time field to indicate when the object was captured; and

storing the tag in a database, wherein the tag indexes a captured object in storage**, the tag being stored to allow subsequent searching for the tag based on one or more of the fields, wherein a tag signature is generated based on the tag, and wherein the object and the tag signature are evaluated to verify if they have been modified since original storage**.

2. (Previously Presented) The computer readable medium of claim 1, wherein the plurality of content types comprises JPEG, GIF, BMP, TIFF, PNG, Skintone, PDF, MSWord, Excel, PowerPoint, MSOffice, HTML, WebMail, SMTP, Telnet, Rlogin, FTP, Chat, GZIP, ZIP, TAR, C++

Source, C Source, FORTRAN Source, Verilog Source, C Shell, K Shell, Bash Shell, Plaintext, Crypto, LIF, Binary Unknown, ASCII Unknown, and Unknown.

3. (Previously Presented) The computer readable medium of claim 1, further comprising generating a device identity field to indicate a device that captured the object.

4. (Previously Presented) The computer readable medium of claim 1, further comprising generating a protocol field to indicate the protocol that carried the object.

5. (Previously Presented) The computer readable medium of claim 1, further comprising an instance field to indicate a number of the object in a connection.

6. (Previously Presented) The computer readable medium of claim 1, further comprising generating an encoding field to indicate a how the object was encoded.

7. (Previously Presented) The computer readable medium of claim 1, further comprising generating a size field to indicate the size of the object.

8. (Previously Presented) The computer readable medium of claim 1, further comprising generating an owner field to indicate an entity that requested capture of the object.

9. (Previously Presented) The computer readable medium of claim 1, further comprising generating a capture rule field to indicate a rule that triggered capture of the object.

10. (Previously Presented) The computer readable medium of claim 1, further comprising generating a signature field to store a signature of the object.

11. (Previously Presented) The computer readable medium of claim 10, wherein the signature comprises a digital cryptographic signature.

12. (Previously Presented) The computer readable medium of claim 1, further comprising generating a tag signature field to store a signature of the data structure.

13. (Previously Presented) The computer readable medium of claim 12, wherein the tag signature comprises a digital cryptographic signature.

14. (Currently Amended) A computer readable medium having stored thereon data representing instructions that, when executed by a processor, cause the processor to perform operations comprising:

storing data associated with capture of an object by a capture system to create a tag that indexes the captured object in storage, ~~wherein the object is captured and the captured object is a plurality of packets that are broken down by the capture system and then reassembled~~ the data comprising:

an Ethernet controller MAC address of the capture system that captured the object;

a source Ethernet IP address of the object;

a destination Ethernet IP address of the object;

a source TCP/IP port number of the object;

a destination TCP/IP port number of the object.

an IP protocol that carried the object when captured by the capture system;

a canonical count of a number of the object within a TCP/IP connection;

a content type of the object;

an encoding that was used on the object;

a size of the object;

a timestamp indicating when the capture system captured the object;

a user who requested capture of the object;

a capture rule that directed capture of the object;

a hash signature of the object; and

a hash signature of the tag**, the tag being stored to allow subsequent searching for the tag based on one or more of the fields, wherein the signatures are evaluated to verify if they have been modified since original storage**.

15. (Previously Presented) The computer readable medium of claim 14, wherein the hash signature of the object comprises a digital cryptographic signature of the object.

16. (Previously Presented) The computer readable medium of claim 15, wherein the hash signature of the tag comprises a digital cryptographic signature of the tag.

17. (Previously Presented) The computer readable medium of claim 14, wherein the content type of the object is one of JPEG, GIF, BMP, TIFF, PNG, Skintone, PDF, MSWord, Excel, PowerPoint, MSOffice, HTML, WebMail, SMTP, Telnet, Rlogin, FTP, Chat, GZIP, ZIP, TAR, C++ Source, C Source, FORTRAN Source, Verilog Source, C Shell, K Shell, Bash Shell, Plaintext, Crypto, LIF, Binary Unknown, ASCII Unknown, and Unknown.

18. – 25. (Canceled)

26. (Currently Amended) A method to index a captured object, comprising:

generating for storage of objects captured during transmission from an origination address to a destination address:

a source address field to indicate an origination address of the object;

a destination address field to indicate a destination address of the object;

a source port field to indicate an origination port of the object;

a destination port field to indicate a destination port of the object;

a content field to indicate a content type from a plurality of content types identifying a type of content contained in the object~~, wherein the object is captured and the captured object is a plurality of packets that are broken down by a capture system and then reassembled~~; and

a time field to indicate when the object was captured; and

storing data in the fields to create a tag, the tag indexing a captured object in storage**, the tag being stored to allow subsequent searching for the tag based on one or more of the fields, wherein a tag signature is generated based on the tag, and wherein the object and the tag signature are evaluated to verify if they have been modified since original storage**.

27. (Currently Amended) A method to index a captured object, comprising:

storing data associated with capture of an object by a capture system to create a tag indexing the captured object in storage, ~~wherein the object is captured and the captured object is a plurality of packets that are broken down by the capture system and then reassembled,~~ the data comprising:

an Ethernet controller MAC address of the capture system that captured the object;

a source Ethernet IP address of the object;

a destination Ethernet IP address of the object;

a source TCP/IP port number of the object;

a destination TCP/IP port number of the object;

an IP protocol that carried the object when captured by the capture system;

a canonical count of a number of the object within a TCP/IP connection;

a content type of the object;

an encoding that was used on the object;

a size of the object;

a timestamp indicating when the capture system captured the object;

a user who requested capture of the object;

a capture rule that directed capture of the object;

a hash signature of the object; and

a hash signature of the tag**, the tag being stored to allow subsequent searching for the tag based on one or more of the fields, wherein the signatures are evaluated to verify if they have been modified since original storage**.